Employer Newsletter: Cyber Security - Phishing Scams Using YOUR Information

From: Missouri Department of Economic Development <MODED@public.govdelivery.com>

Subject: Employer Newsletter: Cyber Security - Phishing Scams Using YOUR Information

Cybercriminals are out there posing as legitimate employers targeting job seekers, using your company information. This Phishing Scam occurs when a scammer "borrows" your FEIN and other information to make a job offer in an attempt to acquire sensitive or confidential information through an email or text. The offer appears legitimate, so the individual usually responds with the information the scammers are hoping to receive, such as a Social Security number or a bank account number.

Another type of scam to hit companies, both big and small, are scammers sending bogus emails to company employees trying to get sensitive information. Recipients get an email from a boss, supervisor, or even a company CEO, instructing them to hand over a password, change an account number, or send over all of the identifying information for the company's employees. Since the email was spoofed to appear as though it came from the boss, the recipient does as he's instructed.

These recent boss phishing attacks have affected several large well-known companies. The language in these emails is very standard and businesslike, and the requests are plausible. For example, asking a payroll employee to send over all of the company's W2 forms to the boss seems like a very likely request at this time of year. Even worse, the email appears to come from the person requesting it, so the instructions are less likely to be questioned.

While you may not be able to prevent an employee from falling for this type of scam and sending your stored information to an identity thief or scammer, there are some things you can do to keep your company safe. If you ever receive any request—logical or otherwise—to send highly sensitive data to someone who requests it, remember these two steps:

- Verify it with the person who requested it using the company-approved contact.
- Use a new email – Don't hit Reply to this type of message. If you're copy/pasting or attaching highly sensitive information, even if you verified it, it's a good idea to initiate a new email with an approved email address.

It's important to note that there's a difference between spoofing the boss' email account and actually taking it over. If the supervisor or CEO's email account was actually hacked, then even a new email message would end up in the scammer's hands. That's why verifying the request (preferably through another means other than email) is a safe bet. If you call the boss and he knows nothing of the information request, there's an excellent chance his email account was actually infiltrated instead of just spoofed.

Taking the steps now to minimize or prevent a phishing attack is a whole lot easier than trying to clean up the damage created by one later.

Phishing Attack Prevention

Be sure to visit our EMPLOYER EVENTS page for the latest information on upcoming sponsorship and participation opportunities for job fairs, as well as other hiring and HR informational meetings.